NEW ENHANCED TECHNIQUES FOR DATA HIDING

Synopsis

Swami Ramanand Teerth Marathwada University,
School of Computational Science
Vishnupuri,Nanded –431606

FOR THE AWARD OF THE DEGREE OF

DOCTORATE in COMPUTER SCIENCE

BY

Dipika Hanmant Deshmukh

Under the guidance of

Dr. G.D.KURUNDKAR
Assistant Professor
Guru Buddhiswamy College,Purna

Content

- **Abstract ……Error! Bookmark not defined.**
- **Introduction ----------Error! Bookmark not defined.**
- **Review on Literature and Development in the subject ----------3-4**
- **Objectives of Research ---------- 4-5**
- **Methodology to be adopted ---------- 5-6**
- **Importance of study/ Society application ----------6**
    - **International status ----------6**
    - **National Status ----------6-7**
    - **Significance of the study ----------7**
- **Proposed work Plan ----------7**
- **References ----------7-8**

1. Introduction

Nowadays security of private information is a major issue over the internet. Because in today's digitized world, the whole communication is done through internet and transferring private data from one end to another using various applications such as e-mails, chats, etc. but there is main issue that is how to protect our confidential information from hackers or cyber criminals over internet. To solve such problems and to maintain the security of data, we should follow an algorithm which should not only encrypt the data into another form but also hides its presence and video steganography helps to provide such a secure environment over internet.

To protect the private information from being misused by the attackers and to overcome the alteration of information, a novel data hiding approach is used. Here we are dealing with video steganography. Video steganography is a process of hiding the secret information behind video bit streams. The main goal of video steganography is to hide presence of secret message from human visual system. Various companies and organizations are following this concept to secure their confidential information and databases from intruders. Video files can hide large amount of hidden data behind their bit streams than images. So, that why they are more preferable than image Steganography [1].

The goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly[2].

2. Review of Literature

Feng Pan et.al has proposed an enhanced version of motion vector based video steganography algorithm by concealing data in motion vectors of cover media. This algorithm has maintained embedding capacity of 4 bits of secret message per 6 motion vectors i.e. approximately 2/3 of total number of motion vectors and PSNR value of more than 30dB. Due to low computational complexity and high bit rate of watermark channel Least Significant bit (LSB) is high used to embed secret data in steganography algorithm [15].

Kousik Dasgupta, J.K. Mandal and Paramartha Dutta has proposed a secured hash based LSB technique for video steganography uses cover video files in spatial domain to hide the presence of sensitive data regardless of its format. Performance analysis of the hash based LSB technique after comparison with LSB technique is quite better [16].

Daniel Socek et.al has proposed an extended version of encryption algorithm of video which is applicable on both lossy and lossless low motion video codec and extension to this encryption

algorithm as a new steganography algorithm to disguise a video inside a video with high security and low computational cost. There are two main types of video encoding standards i.e. compressed and uncompressed [15].

Bin Liu et.al has proposed compressed video secure steganography algorithm to achieve high security with robustness against statistical attacks without decompression process. Run level pairs which are formed by quantization of 8X8 discrete cosine transformed (DCT) are selected as positions to embed secret bits. Video steganography is famous due to high spatial and temporal redundancy. This feature can be easily applied to a steganography algorithm with high security and high embedding efficiency [15].

M.Jafar et.al has proposed a compressed video steganography using temporal and spatial features of video signal. The proposed algorithm has constant bit rate, high imperceptibility and embedded data has been extracted without full decomposition. There are many video steganography schemes proposed on motion vectors as they are used to remove temporal redundancies in video frames [15].

Paul, Acharya et al proposed a Least Significant (LSB) replacement technique using a video steganography in which the secret video is embedded in the original video by creating an index based chaotic sequence and then arranging the pixels according to the sequence. The major advantage of this technique is that there is no perceptual difference between the original video and stego video [17].

Kelash et al proposed a steganographic algorithm based on color histogram has the ability to hide large size of data without any error and provides a high level of authentication to guarantee integrity of video. The advantage of using this technique is that it provides a high security and resistance against attackers [17].

R.Mritha has proposed a modified least significant algorithm for video steganography with high security. Significant growth of video data over internet had made it a popular choice for steganography. Embedding capacity and embedding efficiency are contrary to each other. Maintaining security along with high embedding capacity in steganography is a difficult task [15].

Swathi et.al has proposed a method of video steganography using selection of embedding location by applying polynomial equations. Speed of data extraction and data embedding depends on the steganography algorithm [15].

SUNEETHA et.al has proposed in his work Cryptography and Steganography together system based on hiding data in video by encrypting it with ASCII code and provides a additional layer of security to existing system [16].

3. Objectives

(i)To study the different steganographic techniques

(ii) Find the best data hiding technique.
(iii) To improve the security of the data hiding techniques.
(iv) To provide extra secrecy layer using RSA encryption for the data.
(v) Evaluate the performance of proposed technique by applying the different measures.

4. Methodology

- **Edge detection**

Edge detection is a problem of fundamental importance in image analysis. In typical images, edges characterize object boundaries and are therefore useful for segmentation, registration, and identification of objects in a scene. Edge detection of an image reduces significantly the amount of data and filters out information that may be regarded as less relevant, preserving the important structural properties of an image [6].

- **LSB**

LSB is one of the oldest and most famous substitution-based techniques. In spite of its simplicity, it is capable of hiding large secret messages. It operates by replacing some LSBs of pixels from the cover video with the secret message bits [12].

- **RSA Encryption**

RSA Encryption: To make our secret message more secure, we are using RSA asymmetric key based encryption algorithm. It converts the secret message in an unreadable format and increases its security from hackers. In our work, we have used RSA encryption algorithm instead of symmetric key based encryption. The reason behind this is as the symmetric key based algorithms such as XOR encryption, AES, DES etc. are not secure enough because secret key is always shared with third party members and their security depends on the trustworthy nature of member, and can be easily breakable by attackers. But there is no need of third party member to share secret key between sender and receiver because both sender and receiver are using their own public and private keys to encrypt and decrypt the secret message and also used and large factorial number for encryption, which is hard to decrypt by attackers. So RSA encryption provides high security to our algorithm for hiding the encrypted secret message behind video frames [1].

- **Spatial Domain Methods**

Spatial Domain Methods basically deals with hiding information in pixels of video frames. The most popular method of steganography is Least Significant Bit method (LSB) due to its high embedding capacity, less embedding complexity and ease in implementation .Least Significant method performs embedding of secret message in least significant or most significant bit by randomly selecting pixel from a digital image or a digital video frame [15].

- **Transform techniques**

Transform techniques embed the message by modulating coefficients in a transform domain, such as the *Discrete Cosine Transform* (DCT) used in JPEG compression, *Discrete Fourier Transform*, or *Wavelet Transform*. These methods hide messages in significant areas of the *cover-image,* which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants [2].

- **Format Based Method**

Various techniques have been designed for a particular video format. H.264/AVC is latest video compression standard with high efficiency in compression and well adaptation for network transmission. Due to simple structure and small size Flash Video (.FLV) format video files are considered to be very popular on internet [15].

- **Spread spectrum**

A spread spectrum technique satisfies most requirements and is especially robust against statistical attacks, since the hidden information is scattered throughout the image, while not changing the statistical properties [10].

5. Society application

In current there are many applications for digital steganography of video including

- ✓ Copyright protection
- ✓ Feature tagging
- ✓ Secret communication
- ✓ E-commerce transactions
- ✓ Most users are protected by a username and password, with no real method of verifying that the user is the Actual card holder
- ✓ Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open e-commerce transaction verification [10]

- ➢ **International Status**

- ✓ In the business world steganography can be used to hide a secret chemical formula or plans for a new invention
- ✓ Potential capability to hide the existence of confidential data
- ✓ Hardness of detecting the hidden (i.e., embedded) data
- ✓ Strengthening of the secrecy of the encrypted data[3]

- ➢ **National Status**

Military communications system make increasing use of traffic security technique which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its

receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections [2].

- **Significance of the study**

- ✓ Confidential communication and secret data storing
- ✓ Protection of data alteration
- ✓ Access control system for digital content distribution
- ✓ Media Database systems

6. Proposed Work Plan

Phase 1: Study of existing techniques used in video steganography.
Phase 2: Study of different video steganography methods.
Phase 3: Implementation of selected methods.
Phase 4: Result, Analysis, Interpretation.
Phase 5: Report Writing

7. References

1) Ramandeep Kaur,Pooja,Varsha , **A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques,** IEEE WiSPNET 2016 conference(pp 867-871)

2) Muhalim bin Mohamed Amin, Puan Subariah Ibrahim, Puan Mazleena Salleh,Mohd Rozi Katmin,**Information Hiding Using Steganography** *Vol 71847 Information Hiding using Steganography Approach,2003* (pp 1, 2, 11, 12)

3) Eiji Kawaguchi, et al: A Model of Anonymous Covert Mailing System Using Steganographic Scheme, in **Information Modelling and Knowledge Bases XIV,**H. Yaakkola et al (Eds),IOS Press,2003 (pp 81-85)

4) Mehdi Hussain and Mureed Hussain, **A Survey of Image Steganography Techniques,** International Journal of Advanced Science and Technology Vol. 54, May, 2013(pp 116-118)

5) Rengarajan Amirtharajan, Jiaohua Qin and John Bosco Balaguru Rayappan, **Random Image Steganography and Steganalysis: Present Status and Future Directions**. Information Technology Journal,2012(pp 566-576)

6) Nitin Jain, Sachin Meshram, Shikha Dubey,**Image Steganography Using LSB and Edge – Detection Technique,**International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012 (pp 218)

7) Dipesh Agrawal, **Analysis of Random Bit Image Steganography Technique**,International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013)(pp 1)

8) Pradeep Kumar Saraswat1 and Dr. R. K. Gupta, **A Review of Digital Image Steganography**,Journal of Pure and Applied Science & Technology Copyright © 2011 NLSS, Vol. 2(1), Jan 2012(pp98-106)

9) T Morkel, JHP Eloff and MS Olivier, **An Overview of Image Steganography,***in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandton, South Africa, June/July 2005

10) Masud Karim, S.M. ; Rahman, M.S. ; Hossain, M.I.**A new approach for LSB based image steganography using secret key** Computer and Information Technology (ICCIT), 2011 14th International Conference on Digital Object Identifier: 10.1109/ICCITechn.2011.6164800 Publication Year: 2011(pp 286 – 291)

11) Weiqi Luo ; Fangjun Huang ; Jiwu Huang **Edge Adaptive Image Steganography Based on LSB Matching Revisited** Information Forensics and Security, IEEE Transactions on Volume: 5 ,Issue: 2Digital Object Identifier: 10.1109/TIFS.2010.2041812 Publication Year: 2010 , (pp 201–214)

12) Anil et al., **A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique**, International Journal of Advanced Research in Computer Science and Software Engineering 3(7), July - 2013 (pp 363-372)

13) Gandharba Swain et al, **A Better RGB Channel Based Image Steganography Technique,** Global Trends in Information Systems and Software Applications Communications in Computer and Information Science Volume 270, 2012,(pp 479-488)

14) Sukhpreet Kaur, Sumeet Kaur, **An Image Steganography Approach Based upon Matching ,** High Performance Architecture and Grid Computing Communications in Computer and Information Science Volume 169, 2011,(pp 603-608)

15) Bharti Chandel, Dr.Shaily Jain , **Video Steganography: A Survey**, IOSR Journal of Computer Engineering, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016) (pp 11-17)

16)Pooja Shinde,Tasneem Bano Rehman, **A Novel Video Steganography Technique**, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 12, December 2015 ISSN: 2277 128X (pp 676-684)

17) Heena Goyal et.al, **An Analytical Study on Video Steganography Techniques**, International Journal of Advanced Research in Computer Science, Volume 6, No. 5, May - June 2015(pp 50-52)

Signature

Research Scholar

Signature

Research Guide